Computer Virus Response Using Autonomous Agent Technology

Changing the Paradigm

Christine M. Trently

ctrently@mitretek.org

Outline

0 **Brief Perspective on Computer Virus Response**

0 **Overview of Autonomous Agent Technology**

0 **Agents for Computer Virus Response**

0 **Example Using Agents for Virus Response**

0 **Comparison - Current versus Future**

0 **Future Considerations**

0 **Conclusions**

Brief Perspective - Computer Virus Response

0 **Viruses ?**

0 **Current Response**

0 **Trends**

0 **Need for Change**

0 **Automated Response**

Autonomous Agent (AA) Technology

0 **Agent Characteristics**

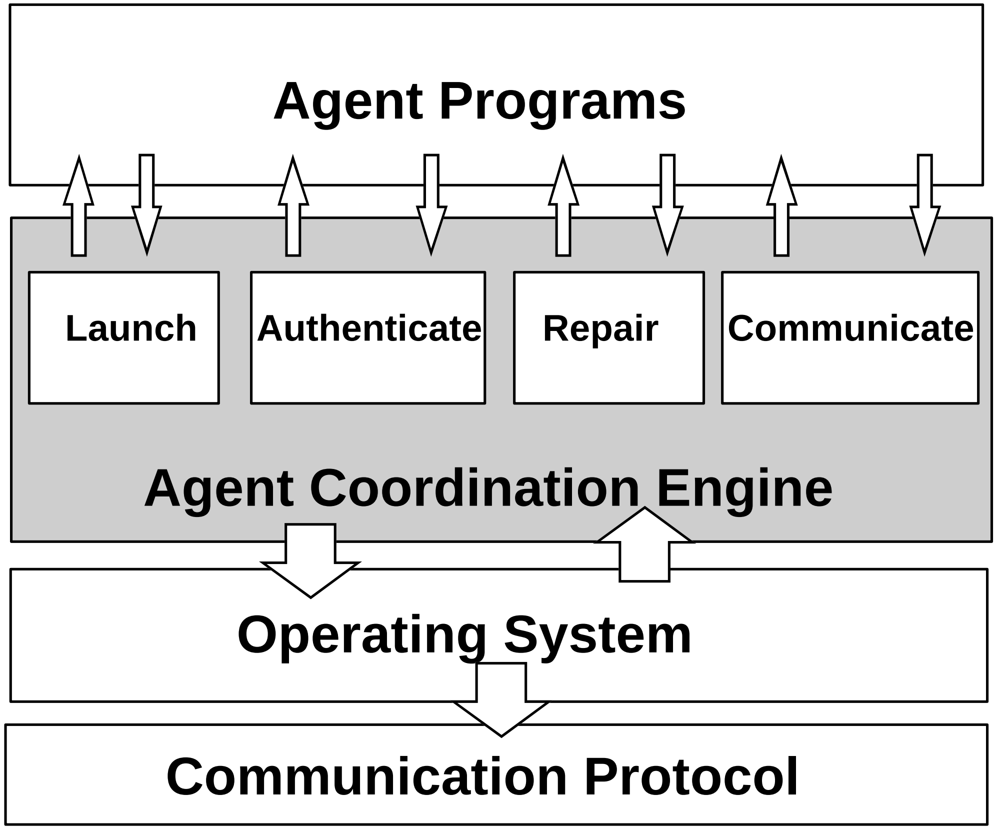
- **Simple, singular task**
- **Mobile**
- **Intelligence - Reasoning**
- **Cooperation**

0 **Operating Environment**

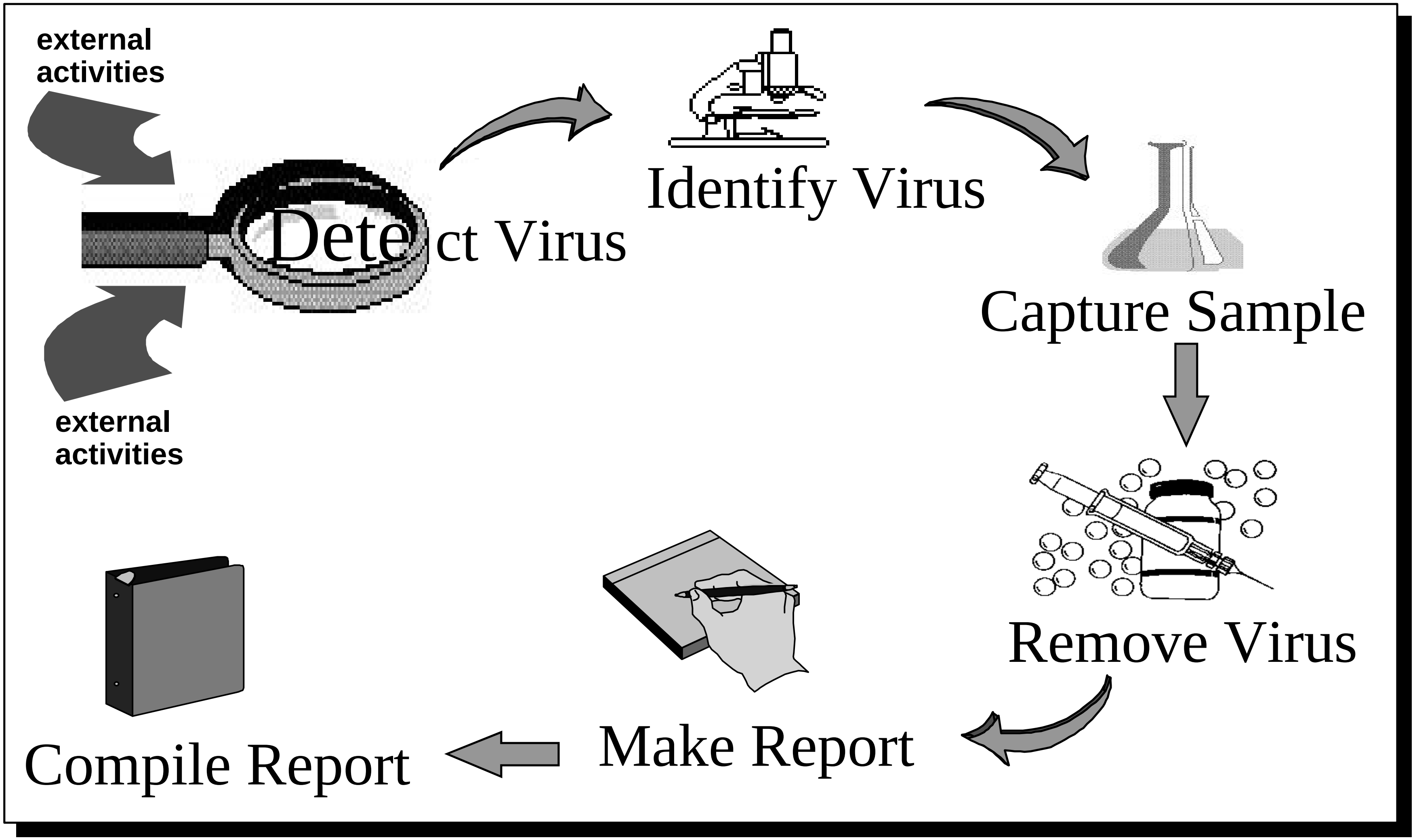
Autonomous Agent (AA) Technology (concluded)

0 Agent Coordination Engine (ACE)

- Launch
- Authenticate
- Repair
- Communicate



The Agents of Virus Response



external activities

external activities

Detect Virus

Identify Virus

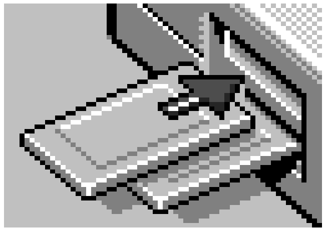
Capture Sample

Remove Virus

Make Report

Compile Report

Responding to Boot Sector Virus Using Agents



0 **Detect**

- **Trigger: Insertion of diskette**
- **Activity: Check for boot sector virus on diskette**
- **Notification: Virus found message sent to ACE**

0 **Identify**

- **Trigger: ACE**
- **Activity: Identify virus detected or**
  Verify (virus) signature from detection
- **Notification: Virus identification to ACE**

0 **Sample**

- **Trigger: ACE**
- **Activity: Make copy of Boot sector / disk image**
- **Notification: Virus sample sent to repository and completion status sent to ACE**

Response for Boot Sector Virus Using Agents (concluded)

0 **Recovery**

- **Trigger: ACE**
- **Activity: Remove virus from boot sector using appropriate technique**
- **Notification: Completion status to ACE**

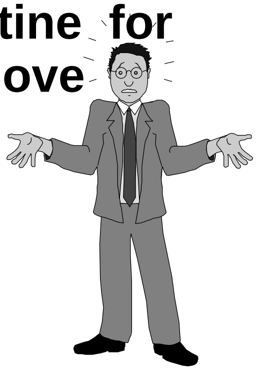
0 **Report**

- **Trigger: ACE**
- **Activity: Generate incident report**
- **Notification: 1) Report sent to administrator;**
  2) Report sent to repository
  3) Completion status to ACE

Virus Response - Comparison
Current vs. Future

0 **Current (User Activity)**

- **Scan computer periodically**
- **Notified by AVS that BS virus detected**
- **Boot from known clean, write-protected diskette**
- **Take a sample by inserting new diskette**
- **Use Recovery diskette or Run Clean-Up routine for given virus to remove virus**
- **Re-scan**
- **Return to Work**



0 **Future (Agent Activity)**

- **Activity on computer is checked by agents**
- **BS virus found on diskette inserted into computer**
- **Virus identified, if applicable**
- **Sample taken**
- **Virus removed**
- **Report generated and administrator notified**

Future Considerations and Conclusions

0 **Reduce Processing Overhead**

0 **Prevent Misuse**

0 **Maintain Agent Integrity**

0 **Identify Target Response**

0 **Provide Identification and Recovery Techniques**

---

0 **Changing the Paradigm**

0 **Providing a loaded gun**